

REMARKS

The Examiner is thanked for the performance of a thorough search. Claims 1-4, 18-21, 32-35, 44, and 45 are amended. No claims are cancelled. New Claims 46 and 47 have been added. Hence, Claims 1-47 are now pending in the application. The amendments to the claims as indicated herein do not add any new matter to this application. Furthermore, amendments made to the claims as indicated herein have been made to exclusively improve readability and clarity of the claims and not for the purpose of overcoming alleged prior art. Each issue raised in the Office Action mailed June 19, 2007 is addressed hereinafter.

Paragraphs [0071], [0082], [0092], [0095] and the heading following paragraph [0101] are amended to correct typographical errors. No new matter has been introduced.

I. ISSUES NOT RELATING TO PRIOR ART

A. Claim Objections

The Office action objected to claims 1-4, 18-21, 32-35, 44, and 45 regarding the word “if.” The objection is respectfully traversed. Present claims 1-4, 18-21, 32-35, 44, and 45 use the term “when” as an equivalent alternative to “if”. Reconsideration is respectfully requested.

B. Claim Rejections - 35 U.S.C. § 101

Claim 44 stands rejected as allegedly presenting non-statutory subject matter under 35 U.S.C. § 101. The rejection is respectfully traversed.

The Office Action contended that the subject matter recited by claim 44 may encompass transmission media subject matter (i.e. electromagnetic carrier signal). Transmission media, such as an electromagnetic wave, are not computer readable storage media because computer-readable instructions cannot be stored on a wave; at best, a wave may temporarily carry instructions, which when stored on a computer-readable storage medium, may be read by a processor. For clarification purposes only, present claim 44 recites a computer readable **storage** medium and thus excludes “transmission” media. Reconsideration is respectfully requested.

II. ISSUES RELATING TO PRIOR ART

Each of the pending claims as amended recites at least one element that is not disclosed, taught, or otherwise suggested by the cited art, either individually or in combination.

Accordingly, the rejections are respectfully traversed.

A. Independent Claim 1

Claim 1 stands rejected under 35 U.S.C. § 102(e) as allegedly unpatentable over *de Silva et al.* (US 6,615,347), hereinafter “*de Silva*”. Claim 1 as currently amended recites:

comparing *in memory* a binary representation of the entire second security certificate to a binary representation of the entire first security certificate;
and
confirming the sender's identity only when the *binary representation of the second security certificate* matches the *binary representation of the first security certificate* for the sender.

(Emphasis added.) Support for the present amendments to Claim 1 are found at least in paragraphs [0102] and [0103] of Applicants' specification. *de Silva* does not teach or otherwise suggest the features emphasized above for at least the following reasons.

de Silva is limited to using the data contained within the digital certificate (e.g., signed hash and/or serial number) to determine whether an existing digital certificate has been changed (see *de Silva*, Col. 6, lines 51-55; Col. 8, lines 6-15; Col. 9, lines 12-19.) Accordingly, the arrangement described by *de Silva* requires advance knowledge of the digital certificate's data structure in order to access and parse the certificate serial number and/or signed hash (i.e., digital signature.) The data structure of the digital certificate referred to by *de Silva* is based on standard X.509 digital certificate formats as is shown in FIG. 2 of *de Silva*; items 202, 214; and also described in the specification at Col. 5, lines 5-10; lines 36-41.

An X.509 certificate includes the following relevant components: Certificate; Version; Serial Number; Algorithm ID; Issuer; Validity; Not Before (Validity Start Date), Not After (Validity Expiration Date); Public Key Info; Public Key; Certificate Signature Algorithm; Certificate Signature. Col. 5, lines 15-41. (A brief summary of the contents of a X.509 formatted digital certificate is available at <http://en.wikipedia.org/wiki/X.509> under “Structure of a digital certificate.”)

However, Applicant’s arrangement as defined by Claim 1 is independent of the received digital certificate’s data structure or the aforementioned X.509 digital certificate standards. The arrangement of Claim 1 compares a binary representation of the entire received digital certificate (i.e., non-hashed) to an existing digital certificate in memory bit-by-bit (i.e., a bitwise operation) to detect changes between the existing and received digital certificates. This approach eliminates certificate format requirements, reduces a step without loss of functionality, is simpler to program and is inherently more secure since more binary information is being compared than using the signed hash method described in *de Silva* at Col. 6, lns.10-13 (See <http://en.wikipedia.org/wiki/X.509> under “Security.”)

Accordingly, since *de Silva* does not teach or otherwise suggest the limitations of comparing binary representations of the entire received digital certificate to an existing digital certificate in memory, Claim 1 is therefore novel and non-obvious. Applicant respectfully requests reconsideration and withdrawal of Examiner’s anticipation rejection of Claim 1.

B. Independent Claims 18 and 32

Independent Claims 18 and 32 recite features analogous to those provided in amended Claim 1. Claims 18 and 32 further include the limitation of “*without parsing of data fields contained within either the first or second security certificates.*” (Emphasis added.) Support for this amendment is found in Applicant’s specification at least in paragraph [0102]. This feature is not taught or otherwise suggested by *de Silva*.

de Silva is limited to using the data contained within the digital certificate (e.g., signed hash and/or serial number) to determine whether an existing digital certificate has been changed (see *de Silva*, Col. 6, lines 51-55; Col. 8, lines 6-15; Col. 9, lines 12-19.) In contrast, claims 18 and 32 recite processes that **do not use data within the digital certificate**—"without parsing of data fields contained within ... certificates." *de Silva* has no suggestion not to use data in the digital certificate. Claims 18 and 32 are patentably distinct from *de Silva* obvious at least for the reasons discussed above for Claim 1. The additional feature quoted above further renders Claims 18 and 32 novel and non-obvious over *de Silva*. Reconsideration is respectfully requested.

C. Independent Claims 44 and 45

Independent Claims 44 and 45 recite features analogous to those provided in amended Claim 1. Since *de Silva* does not teach or otherwise suggest the limitations of comparing binary representations of the entire received digital certificate to an existing digital certificate in memory, Claims 44 and 45 are patentable over *de Silva* for the same reasons given above with respect to claim 1. Reconsideration is respectfully requested.

Certain other amendments to Claims 44 and 45 address grammatical issues only and were not made for reasons related to patentability.

D. Dependent Claims 2-17, 19-31, 33-41 and 43

Claims 2-17, 19-31, 33-41 and 43 stand rejected under 35 U.S.C. § 102(e). Claims 2-17, 19-31, 33-41, depend directly or indirectly from Claims 1, 18, 32, 44, 45 and therefore include each and every feature recited in independent Claims 1, 18, 32, 44, 45. Accordingly, claims 2-17, 19-31, 33-41 and 43 are allowable for the same reasons given above for claims 1, 18, 32, 44, 45. Reconsideration is respectfully requested.

E. Dependent Claim 42

Claim 42 stands rejected under 35 U.S.C. § 103 (a) as allegedly obvious over *de Silva* in view of US patent application publication US 2003/0037234 to *Fe et al.*

Claim 42 depends from independent Claim 32 and therefore includes each and every feature recited in claim 32. For the reasons given above, claim 32 is patentable over *de Silva*.

Further, *Fe et al.* fails to cure the deficiencies of *de Silva* with respect to the distinguishing features of claim 32—in particular, *Fe et al.* has no description, teaching or suggestion to perform the claimed process without using data in the digital certificate. Therefore, any combination of *de Silva* and *Fe et al.* fails to provide for the complete combination that is recited in claim 42. Reconsideration is respectfully requested.

F. Dependent Claims 46 and 47

New dependent Claim 46 provides an additional comparison feature which utilizes the length in memory of the first and second digital certificates to determine whether any changes have occurred. Support is found in Applicant's specification at least at paragraph [103].

New dependent Claim 47 provides the feature incorporated into independent Claims 18 and 32 which affords comparisons of the first and second digital certificates without having to parse the individual data fields contained within the digital certificates. Support is found in Applicant's specification at least at paragraph [102].

New Claims 46 and 47 depend from independent Claim 45 and therefore include each and every feature recited in Claim 45. Claim 45 recites the same features discussed above for claim 1 and therefore claim 45 is patentable over the cited references for the same reasons given above for claim 1. Accordingly, dependent Claims 46 and 47 are patentable over *de Silva* for the same reasons given above for claim 1 and also because the additional features recited in claim 46 and claim 47 are not found in *de Silva*. Favorable consideration is respectfully requested.

III. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, the petition for extension of time fee and other applicable fees are submitted concurrently herewith. If any applicable fee is missing or insufficient, throughout the

pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

/ChristopherJPalermo#42056/
Christopher J. Palermo
Reg. No. No. 42,056

Dated: September 19, 2007

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
(408) 414-1202
Facsimile: (408) 414-1076